# Substituição de WLAN + VLAN 802.1x com Mobility Express (ME) 8.2 e ISE 2.1

# Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Configurar Diagrama de Rede Configurações Configuração em ME Declarar-me no ISE Criar um novo usuário no ISE Criar a regra de autenticação Criar a regra de autorização Configuração do dispositivo final Verificar Processo de autenticação em ME Processo de autenticação no ISE

# Introduction

Este documento descreve como configurar uma WLAN (Wireless Local Area Network) com segurança empresarial Wi-Fi Protected Access 2 (WPA2) com um controlador Mobility Express e um servidor Remote Authentication Dial-In User Service (RADIUS). O Identity Service Engine (ISE) é usado como exemplo de servidores RADIUS externos.

O EAP (Extensible Authentication Protocol) usado neste guia é o PEAP (Protected Extensible Authentication Protocol). Além disso, o cliente é atribuído a uma VLAN específica (diferente daquela atribuída ao padrão da WLAN).

# Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- 802,1x
- PEAP
- Autoridade de certificação (CA)
- Certificados

### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

ME v8.2

ISE v2.1

Notebook Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Configurar

Diagrama de Rede



#### Configurações

As etapas gerais são:

- 1. Crie o Service Set Identifier (SSID) no ME e declare o servidor RADIUS (ISE neste exemplo) no ME
- 2. Declarar-me no servidor RADIUS (ISE)
- 3. Criar a regra de autenticação no ISE
- 4. Criar a regra de autorização no ISE
- 5. Configurar o endpoint

#### Configuração em ME

Para permitir a comunicação entre o servidor RADIUS e ME, é necessário registrar o servidor RADIUS em ME e vice-versa. Esta etapa mostra como registrar o servidor RADIUS em ME.

Etapa 1. Abra a GUI do ME e navegue até Configurações sem fio > WLANs > Adicionar nova



Etapa 2. Selecione um nome para a WLAN.

Add Ne	ew WLAN		×
General	WLAN Security	VLAN & Firewall	QoS
	WLAN Id	3 •	
	Profile Name *	me-ise	
	SSID *	me-ise	
	Admin State	Enabled 🔹	
	Radio Policy	ALL .	
		🛛 Арр	ly 🛞 Cancel

Etapa 3. Especifique a configuração de segurança na guia WLAN Security.

Escolha **WPA2 Enterprise**, para Servidor de autenticação, escolha **RADIUS externo**. Clique na opção de edição para adicionar o endereço ip do RADIUS e selecionar uma chave **secreta compartilhada**.



Add N	ew WLAN	×
General	WLAN Security	VLAN & Firewall QoS
Authe	Security ntication Server	WPA2 Enterprise  • External Radius  •
<ul> <li>⊘</li> <li></li> <li>&lt;</li></ul>	Radius IP 🛦	Radius Port Shared Secret          1812       •••••••         e enter valid IPv4 address       •••••••
External F all WLANs	Radius configuration a	applies to 🛛 📿 Apply 🛞 Cancel

<a.b.c.d> corresponde ao servidor RADIUS.

Etapa 4. Atribua uma VLAN ao SSID.

Se o SSID precisar ser atribuído à VLAN do AP, essa etapa poderá ser ignorada.

Para atribuir os usuários desse SSID a uma VLAN específica (diferente da VLAN do AP), habilite **Usar marcação de VLAN** e atribua o **ID de VLAN** desejado.

Add New WLAN	×
General WLAN Security	VLAN & Firewall QoS
Use VLAN Tagging	Yes 🔻
VLAN ID *	2400 🔹
Enable Firewall	No 🔻
	c
VLAN and Firewall configuration all WLANs	n apply to 🛛 🖉 Apply 🛞 Cancel

**Note**: Se a marcação de VLAN for usada, certifique-se de que a porta de switch à qual o ponto de acesso está conectado esteja configurada como porta de tronco e a VLAN do AP esteja configurada como nativa.

Etapa 5. Clique em Apply para concluir a configuração.

Add New WLAN	×
General WLAN Security	VLAN & Firewall QoS
Use VLAN Tagging	Yes
VLAN ID *	2400 🔹
Enable Firewall	No 🔹
VI AN and Firewall configuration	
all WLANs	Apply (S) Cancel

Etapa 6. Opcional, configure a WLAN para aceitar a substituição da VLAN.

Ative a substituição de AAA na WLAN e adicione as VLANs necessárias. Para fazer isso, você precisará abrir uma sessão CLI para a interface de gerenciamento do ME e emitir estes comandos:

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
Declarar-me no ISE
```

Etapa 1. Abra o console do ISE e navegue até Administration > Network Resources > Network Devices > Add.

diado Identity Servi	ices Engine Hom	e 🔹 🕨 Context Visibility	▶ Operations → Polic	y ▼Administration → Worl
▶ System → Identi	ity Management 🛛 🕶 Netw	rork Resources 🔹 > Devi	ce Portal Management pxG	rid Services 🔸 Feed Service 🕠
✓Network Devices	Network Device Groups	Network Device Profile	s External RADIUS Server:	s RADIUS Server Sequences
	Ø			
Network devices	Ne	twork Devices		
Default Device	/	Edit 🕂 Add 🕞 Duplicat	e 👍 Import 🕞 Export 👻	ⓓ Generate PAC XDelete ▼

Etapa 2. Inserir informações.

Opcionalmente, ele pode ser especificado como Nome do modelo, versão do software, descrição e atribuição de grupos de dispositivos de rede com base em tipos de dispositivos, localização ou WLCs.

a.b.c.d corresponde ao endereço IP do ME.

Network Devices List > New Network Device Network Devices
* Name WLC-name
Description optional description
* IP Address: a.b.c.d / 32
* Device Profile 🛛 😹 Cisco 👻 🕀
Model Name wic-model
Software Version wic-software 👻
* Network Device Group
Jentee type WLCs-2504
All Locations Set To Default
WLCs 🛛 📀 Set To Default
RADIUS Authentication Settings
Enable Authentication Settings
Protocol RADIUS
* Shared Secret Show
Enable KeyWrap 🗌 👔
* Key Encryption Key Show
* Message Authenticator Code Key Show
Key Input Format 💿 ASCII 🔵 HEXADECIMAL
CoA Port 1700 Set To Default

Para obter mais informações sobre Grupos de dispositivos de rede, consulte este link:

ISE - Grupos de dispositivos de rede

Criar um novo usuário no ISE

Etapa 1. Navegar para Administração > Gerenciamento de Identidades > Identidades > Usuários > Adicionar.

diado Identity Services Engine	Home	▶ Context Visibility	Operations	Policy	<ul> <li>Administration</li> </ul>
▶ System ▼Identity Management	• Network R	esources 🕨 Device	Portal Manageme	nt pxGrid 8	System
■Identities Groups External Ident	iity Sources	Identity Source Sequ	Jences 🔹 🕨 Setting	js	Deployment Licensing
C Users	Network	k Access Users			Certificates Logging Maintenance
Latest Manual Network Scan Res	🥖 Edit 🧧	🕂 Add 🔣 Change St	atus 👻 🅵 Import	Export 👻	Upgrade Backup & Restor
	Statu	us Name	-	Description	Admin Access
	🎲 Loa	ding			Settings
				_	Identity Managem
					Identities

Etapa 2. Inserir informações.

Neste exemplo, este usuário pertence a um grupo chamado ALL\_ACCOUNTS, mas pode ser ajustado conforme necessário.

Network Access Users List > New Network Access User	
Network Access User	
* Name user1	
Status 🛃 Enabled 👻	
Email	
<ul> <li>Passwords</li> </ul>	
Password Type: Internal Users 🔹	
Password	Re-Enter Passw
* Login Password	•••••
Enable Password	
<ul> <li>User Information</li> </ul>	
First Name	
Last Name	
- A construct Outlines	
Account Uptions	
Description	
Change password on next login	
<ul> <li>Account Disable Policy</li> </ul>	
Disable account if date exceeds 2017-01-21	
User Groups	
ALL_ACCOUNTS (default) 📀 🛶 🕂	
Submit Cancel	

#### Criar a regra de autenticação

As regras de autenticação são usadas para verificar se as credenciais dos usuários estão corretas (verifique se o usuário realmente é quem ele diz ser) e limite os métodos de autenticação

que podem ser usados por ele.

Etapa 1. Navegar para Política > Autenticação.



Etapa 2. Insira uma nova regra de autenticação.

Para fazer isso, navegue para Política > Autenticação > Inserir nova linha acima/abaixo.

altalo cisco	Identity Services Engine	Home	▶ Context Visibility	▶ Operations	→ Policy	▶ Administration	▶ Work Centers	L
Auth	entication Authorization	Profiling Pos	ture Client Provisio	ning 🔹 🕨 Policy El	ements			
ting the p System > ed	rotocols that ISE should use to Backup & Restore ≻ Policy Exp	o communicate port Page	with the network device	es, and the identity	sources that it	should use for auther	ntication.	
_Protoco	: If Wired_MAB <b>OR</b> Is and :use Internal Endpoints	3						Insert new row above Insert new row below
IC_Proto	: If Wired_802.1X <b>OR</b> cols and							Duplicate below

#### Etapa 3. Insira as informações necessárias

Este exemplo de regra de autenticação permite todos os protocolos listados na lista **Acesso de Rede Padrão**, que se aplica à solicitação de autenticação para clientes Wireless 802.1x e com ID de Estação Chamada e termina com *ise-ssid*.

dialo Identity	Services Engine	Home	Context Visibility	<ul> <li>Operations</li> </ul>	▼Policy	<ul> <li>Administration</li> </ul>	Work Centers	
Authentication	Authorization	Profiling Postur	e Client Provisioni	ing 🔹 🕨 Policy Ele	ments			
Authenticatio Define the Auther For Policy Export	Authentication Policy Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authenticat For Policy Export go to Administration > System > Backup & Restore > Policy Export Page							
Policy Type 🔿	Simple 💿 Rule	-Based						
1	Rule name	: If	Wireless_802.1X	AND Select Attribu	rte 😐 Ar	low Protocols : Defau	It Network Access	📀 and 🕳
₹.	Default		Je Condition N Wireless_802	ditions Below to L lame [ 2.1X O A c	brary Description Indition to m Radius:Cal	atch 802.1X based au ed-Sta 📀 🛛 Ends	thentication request	AND V AND

Além disso, escolha a origem da identidade para os clientes que correspondem a esta regra de autenticação, neste exemplo ela é usada *por usuários internos* 

Rule name : If Wi	reless_802.1X AND Radius:Call	It Network Access 📀 and .
Default : Use	Internal Users Identity Source Internal Users Options If authentication failed Reject  If user not found Reject  If process failed Drop  Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or  it is not possible to continue processing when authentication fails o If continue option is selected in these cases, requests will be reject	Identity Source List
		Internal Users

#### Depois de concluir, clique em Concluído e Salvar

Rule name	: If Wireless_802.1X AND Radius:Cal If Wireless_802.1X AND Radius:Cal	Done
Default	: Use Internal Users 🗇	Actions 👻
Save		

Para obter mais informações sobre Permitir Políticas de Protocolos, consulte este link:

### Serviço de Protocolos Permitidos

Para obter mais informações sobre fontes de identidade, consulte este link:

Criar um grupo de identidade de usuário

#### Criar a regra de autorização

A regra de autorização é a responsável para determinar se o cliente pode ou não ingressar na rede

#### Etapa 1. Navegue até Política > Autorização.

es Engine	Home	) ¢	ontext Visibility	<ul> <li>Operations</li> </ul>	▼Policy	Administration	Work Centers
norization	Profiling P	osture	Client Provisionin	ng 🔹 🕨 Policy Ele	Authentic	ation	Authorization
					Profiling		Posture
V Policy by co dministratio plies	onfiguring rules on > System > E	: based ( Backup &	on identity groups a & Restore > Policy E	ind/or other condi Export Page	Client Pro	wisioning	Policy Elements Dictionaries Conditions Results

Etapa 2. Inserir uma nova regra. Navegue até **Política > Autorização > Inserir nova regra** acima/abaixo.

altala cisco	Identity	Services Engin	e Hon	ne ⊧C	ontext Visibility	<ul> <li>Operations</li> </ul>	→ Policy	Administration	• Work Centers	License \
Authe	ntication	Authorization	Profiling	Posture	Client Provisionin	g + Policy Eleme	ents			
rtiguring ru	les based	on identity groups	and/or other	r conditions	. Drag and drop n	ules to change the	order.			
> System	> Backup 8	Restore > Policy	Export Page							
*										
		Conditions	(identity arou	uns and off	ver conditions)			Permissions		
									_	
										Insert New Rule Above Insert New Rule Below
										Duplicate Above
										Duplicate Below

Etapa 3. Inserir informações.

Primeiro escolha um nome para a regra e os grupos de identidades onde o usuário está armazenado. Neste exemplo, o usuário é armazenado no grupo *ALL\_ACCOUNTS*.

	Status	Rule Name	Co	nditions (identity groups and other conditio	ons) Permissions	
0		NameAuthZrule		Any Pland Condition(s)	💠 then AuthZ	Pr 🗇
	~	75.5	if V			
	<ul> <li>Image: A set of the set of the</li></ul>	Manetes Tablek (391,504m)	if C'	PC Any		less Ac. 55
11	<b>~</b>	Profiled Cases and All a	if C	:	User Identity Groups	s
1	<b>~</b>	Francis Mon Cheo IR Pixerax	if <u>No</u>	n	⟨→ ▼   = ▼ ♀ ♀ ↓	ગલ્લા
	0	Compliant_Devices_Autority	if 🐴	<b>ə</b> t	<ul> <li>GuestType_Daily (default)</li> <li>GuestType Weekly (default)</li> </ul>	
	0	Employee, FAP TI S	if 🕺	ír Sí Maria Ann	GuestType_Contractor (default)	ANE CARACTER
	0	Etipeves Ophoenline i	if QA	freises_803.1Y AND EAP-MSCHAPy2 )	ALL_ACCOUNTS (default)	1002.0X10.
	-				<ul> <li>OWN_ACCOUNTS (default)</li> </ul>	

Depois disso, escolha outras condições que façam com que o processo de autorização se enquadre nessa regra. Neste exemplo, o processo de autorização atinge esta regra se ela usa 802.1x Wireless e é chamada de ID da estação termina com *ise-ssid*.

St	atus	Rule Name	Conditions (id	lentity groups	and other conditions)	Permissions	
1	-	NameAuthZrule	if AL	🗘 and	Wireless_802.1X AND Radius:Call	😑 then AuthZ Pr 💠	
	1			iš	💾 Add All Conditions Below to Librar	У	
				9	Condition Name De	escription	AND -
					Wireless 802.1X 📀 Normali	sed Radius:RadiusFlowType EQUALS Wireless80 tadius:Called-Stat 👩 Ends With 🚽 is:	J2_1> AND e-ssid 📀
				е			

Finalmente, escolha o perfil de autorização que permite que os clientes ingressem na rede, clique em **Concluído** e **Salvar**.

	Status	Rule Name	Conditions (identity	groups and other conditions)	Perm	nissions		
	<b>-</b>	NameAuthZrule	if AL <	and Wireless_802.1X AND Radius:Call	💠 then	PermitAc		Done
1	~					·		Edit   🕶
1						PermitAccess		Edit   🕶
1							Standard	Edit   🕶
1	~							Edit   🕶
1	0						C E	Edit   🕶
1	0							Edit   🕶
-	0						2 C	5-00 I
	0						1	Eat
1	0						PermitAccess	Edit   🕶
1	0							Edit   🕶
1								Edit   +
	<b>~</b>	Default	if no matches, then	DenyAccess				Edit   🕶
	_							
Sa	ve Res	set						

Opcionalmente, crie um novo perfil de autorização que atribua o cliente sem fio a uma VLAN diferente:

•		
(	> - +	
	Standard	
	↓ ■ .	نې چې
	😪 Blackhole_Wireless_Access	🎡 Add New Standard Profile

Inserir informações:

Add New Standard Pro	file		1
Authorization Profile		í	ì.,
* Name	e name-of-profile		
Description			
* Access Type	access_accept		
Network Device Profile	the Cisco 🔹 🕀		
Service Template			
Track Movement			
Passive Identity Tracking	9 D 0		
▼ Common Tasks			
DACL Name		^	
		- 84	
ACL (Filter-ID)			
_			
🗹 VLAN	Tag ID 1 Edit Tag IDName Van-id		
Voice Domain Perm	nission		
		Ŷ	
<ul> <li>Advanced Attribut</li> </ul>	tes Settings		
Select an item			
<ul> <li>Attributes Details</li> </ul>			
Access Type = ACCESS Tunnel-Private-Group-ID Tunnel-Type = 1:13 Tunnel-Medium-Type =	LACEPT D = 1:vbn-id 1:f6		
americanite type -			
C		>	
		Save	ance

#### Configuração do dispositivo final

Configurar um computador portátil Windows 10 para ligar a um SSID com autenticação 802.1x utilizando PEAP/MS-CHAPv2 (versão Microsoft do Challenge-Handshake Authentication Protocol versão 2).

Neste exemplo de configuração, o ISE usa seu certificado autoassinado para executar a autenticação.

Para criar o perfil da WLAN na máquina Windows, há duas opções:

- 1. Instalar o certificado autoassinado na máquina para validar e confiar no servidor ISE para concluir a autenticação
- 2. Ignorar a validação do servidor RADIUS e confiar em qualquer servidor RADIUS usado para executar a autenticação (não recomendado, pois pode se tornar um problema de segurança)

A configuração dessas opções é explicada na <u>configuração do dispositivo final - Create the</u> <u>WLAN Profile - Step 7</u>.

Configuração do dispositivo final - Instalar certificado autoassinado do ISE

Etapa 1. Exportar certificado autoassinado do ISE.

Faça login no ISE e navegue até Administration > System > Certificados > System Certificados.

Em seguida, selecione o certificado usado para a autenticação EAP e clique em Exportar.



Salve o certificado no local necessário. Este certificado está instalado na máquina do Windows.

Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'	×
<ul> <li>Export Certificate Only</li> </ul>	
Export Certificate and Private Key	
*Private Key Password	
*Confirm Password	
Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key	÷γ.
Export	cel

Etapa 2. Instale o certificado na máquina do Windows.

Copie o certificado exportado antes para a máquina do Windows, altere a extensão do arquivo de .pem para .crt, depois de clicar duas vezes nele e selecione **Instalar certificado...**.

👼 Certificate	×
General Details Certification Path	
Certificate Information	
This CA Root certificate is not trusted. install this certificate in the Trusted Ro Authorities store.	To enable trust, oot Certification
Issued to: EAP-SelfSignedCertificate	,
Issued by: EAP-SelfSignedCertificate	,
<b>Valid from 23/11/2016 to 23/11/2</b>	018
Install Certificat	e Issuer Statement
	ОК

Escolha instalá-lo na máquina local e clique em Avançar.

🔶 😸 Certificate Import Wizard	^
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network	
connections. A certificate store is the system area where certificates are kept. Store Location Current User O Local Machine	
To continue, click Next.	
Next Cance	

Selecione Colocar todos os certificados na loja a seguir e, em seguida, navegue e escolha Autoridades de Certificação de Raiz Confiáveis. Depois disso, clique em Avançar.

←	🚰 Certificate Import Wizard	^
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	Automatically select the certificate store based on the type of certificate	
	Place all certificates in the following store	
	Certificate store:	
	Trusted Root Certification Authorities Browse	
	Next Canc	el

V

Em seguida, clique em Concluir.

🗲 🛛 🛃 Certificate Import Wizard	×
Completing the Certificate Import Wizard	
The certificate will be imported after you click Finish.	
You have specified the following settings:	
Certificate Store Selected by User Trusted Root Certification Authorities Content Certificate	
Finish Cano	el:

No final, clique em Sim para confirmar a instalação do certificado.

### Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

### Warning:

If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?



Finalmente, clique em OK.



Configuração do dispositivo final - Criar o perfil da WLAN

Etapa 1. Clique com o botão direito do mouse no ícone Iniciar e selecione Painel de controle.

	Programs and Features
	Mobility Center
	Power Options
	Event Viewer
	System
	Device Manager
	Network Connections
	Disk Management
	Computer Management
	Command Prompt
	Command Prompt (Admin)
	Task Manager
	Control Panel
	File Explorer
	Search
	Run
	Shut down or sign out
	Desktop
ł	ال الع Downi 👳 Networ 👳 N

Etapa 2. Navegue até **Rede e Internet** e, em seguida, para **Central de Rede e Compartilhamento** e clique em **Configurar uma nova conexão ou rede.** 

💐 Network and Sharing Center										
← → ✓ ↑ 💐 > Control Panel > Network and Internet > Network and Sharing Center										
Control Panel Home View your basic network information and set up connections										
Change adapter settings	View your active networks									
Change advanced sharing settings	<b>cisco.com</b> Domain network	Access type: Internet Connections: <i>«</i> Ethernet								
	Change your networking settings Set up a new connection or ne Set up a broadband, dial-up, o Troubleshoot problems Diagnose and repair network p	etwork or VPN connection; or set up a router or access point. problems, or get troubleshooting information.								

Etapa 3. Selecione Conectar manualmente a uma rede sem fio e clique em Avançar.

	_		×
🔶 🛬 Set Up a Connection or Network			
Choose a connection option			
•			
Connect to the Internet			
Set up a broadband or dial-up connection to the Internet.			
Set up a new network			
Set up a new router or access point.			
Manually connect to a wireless network			
Connect to a hidden network or create a new wireless profile.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
	Next	Can	cel

Etapa 4. Insira as informações com o nome do SSID e o tipo de segurança WPA2-Enterprise e clique em **Avançar**.

				_		×
÷	💐 Manually connect to a v	vireless network				
	Enter information fo	r the wireless network you want	to add			
	Network name:	ise-ssid				
	Security type:	WPA2-Enterprise $\vee$				
	Encryption type:	AES				
	Security Key:	Hic	de character	'S		
	Start this connection	automatically				
	Connect even if the	network is not broadcasting				
	Warning: If you sele	ct this option, your computer's privacy mig	ht be at risk			
			N	ext	Cano	:el

Etapa 5. Selecione Alterar configurações de conexão para personalizar a configuração do perfil da WLAN.

	_		×
<ul> <li>Manually connect to a wireless network</li> </ul>			
Successfully added ise-ssid			
-> Change connection settings			
Open the connection properties so that I can change the settings.			
		Clo	se

Etapa 6. Navegue até a guia Segurança e clique em Configurações.

ise-ssid Wireless Ne	twork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		$\sim$	
Encryption type:	AES		$\sim$	
Choose a network au	thentication method:	_	_	
Microsoft: Protected	EAP (PEAP)	Settin	gs	
Remember my cre time I'm logged o	edentials for this connec n	tion each		
Advanced settings	<b>;</b>			
	_			
		ОК	Can	cel

Passo 7. Escolha se o servidor RADIUS é validado ou não.

Em caso afirmativo, habilite Verifique a identidade do servidor validando o certificado e na Lista de autoridades de certificação raiz confiáveis: selecione o certificado autoassinado do ISE.

Depois disso, selecione **Configurar** e desativar **Utilizar automaticamente o nome de início de sessão e a senha do Windows...** e, em seguida, clique em **OK** 

Protected EAP Properties	×								
When connecting:									
Verify the server's identity by validating the certificate									
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):									
Trusted Root Certification Authorities:									
Eggille & Clobel Line and	^								
EAP-SelfSignedCertificate									
<ul> <li>Fortunet Royal Configuration, M. Status, C. S. S.</li> <li>L. M. Schultz Configuration of Configuration, Status, Configuration, Configuratio, Configuration, Configuration, Configuration, Configuratio</li></ul>	~								
< >									
Notifications before connecting:									
Tell user if the server name or root certificate isn't specified	~								
Select Authentication Method:	_								
Secured password (EAP-MSCHAP v2) Configu	re								
C Enable Fast Reconnect									
Disconnect if server does not present cryptobinding TLV									
Enable Identity Privacy									
OK Cano	el								

EAP MSCHAPv2 Properties							
When connecting:							
Automatically use my Windows logon name and password (and domain if any).							
OK Cancel							

### Etapa 8. Configurar as credenciais do usuário

Depois de voltar à guia **Segurança**, selecione **Configurações avançadas**, especifique o modo de autenticação como **autenticação do usuário** e salve as credenciais configuradas no ISE para autenticar o usuário.

ise-ssid Wireless Network Properties X								
Connection Security								
Security type:	WPA2-Enterprise		~					
Encryption type:	AES		$\sim$					
Choose a network au	thentication method:							
Microsoft: Protected	EAP (PEAP) 🗸 🗸	Settin	igs					
Remember my cre time I'm logged o	edentials for this connect n	ion each						
	_							
Advanced settings	•							
		ок	Cancel					

Advanced sett	ings		×
802.1X settings	802.11 settings		
Specify a	uthentication mode:		
User aut	hentication $$	Save credent	tials
Delete	e credentials for all users		
Enable si	ngle sign on for this network		
Perfo	rm immediately before user log	ion	
O Perfo	rm immediately after user logo	n	
Maximun	n delay (seconds):	10	*
Allow sign o	additional dialogs to be display on	ed during single	
This r and u	network uses separate virtual L ser authentication	ANs for machine	
		ОК	Cancel

Windows Secur	ity	Х
Save creden Saving your crea when you're no	tials dentials allows your computer to connect to the network t logged on (for example, to download updates).	
 cisco	user1	
	OK Cancel	

## Verificar

O fluxo de autenticação pode ser verificado a partir da WLC ou da perspectiva do ISE.

Processo de autenticação em ME

Execute este comando para monitorar o processo de autenticação de um usuário específico:

> debug client <mac-add-client>
Exemplo de uma autenticação bem-sucedida (alguma saída foi omitida):

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```

AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client \*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is \*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48) \*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3 \*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1 \*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45 \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth\_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x\_reauth\_sm.c:47 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries \*Dot1x NW\_MsqTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime. \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800 \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dotlx - moving mobile 08:74:02:77:13:45 into Connecting state \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1) \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253 \*Dot1x NW MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800 \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2) \*Dot1x NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: New PMKID: (16) \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent \*Dot1x NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same. \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70) \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45 \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: Including PMKID in M1 (16) \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: M1 - Key Data: (22) \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Starting key exchange to mobile

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45 \*Dot1x NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45 \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dotlx - moving mobile 08:74:02:77:13:45 into Authenticated state \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK\_START state (message 2) from mobile 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!! \*Dot1x NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!! \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0..... \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 ..... \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000000: 01 00 00 of ac 04 01 00 00 of ac 04 01 00 00 Of ..... \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 .... \*Dot1x NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45 \*Dot1x NW MsqTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45 state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45 \*Dotlx NW MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X\_REQD (3) \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce : \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload: \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0 \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224 \*Dot1x NW\_MsqTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1 \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload. \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00 \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name: \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP\_REQD (7) last state L2AUTHCOMPLETE (4) \*Dotlx\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) pemAdvanceState2 6623, Adding TMP rule \*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) Adding Fast Path rule type = Airespace AP - Learn IP address

08:74:02:77:13:45, data packets will be dropped

on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0 IPv4 ACL ID = 255, IPv \*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) mobility role update request from Unassociated to Local Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136 \*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) State Update from Mobility-Incomplete to Mobility-Complete, mobility role=Local, client state=APF\_MS\_STATE\_ASSOCIATED \*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) pemAdvanceState2 6261, Adding TMP rule \*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) Replacing Fast Path rule type = Airespace AP - Learn IP address on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0 IPv4 ACL ID = 255, \*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255) \*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0 \*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0 \*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB ip\_learn\_type 1, add\_or\_delete 1 \*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0 \*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb\_debug: regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller apf\_ms.c:3593) \*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0 \*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB ip\_learn\_type 1, add\_or\_delete 1 \*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP\_REQD (7) Change state to RUN (20) last state DHCP\_REQD (7)

Para uma maneira fácil de ler as saídas do debug client, use a ferramenta *Wireless debug analyzer*.

#### Analisador de depuração sem fio

#### Processo de autenticação no ISE

Navegue até **Operações > RADIUS > Logs ao vivo** para ver qual política de autenticação, política de autorização e perfil de autorização atribuídos ao usuário.

alfalfa cisco	Identit	y Service	is Engine	Home	♦ Context V	isibility 👻	Operations	Policy     ■	► Administra	ation +	Work Centers		License
▼RAI	DIUS	TC-NAC Liv	ve Logs	+ TACACS	Reports + Tr	roubleshoot	▶ Adaptive	Network Contr	ol				
Live L	Logs	Live Sessio	ons										
		ħ	/lisconfigu	ired Supplic	ants Mi	sconfigured Devices	Network Ø	R	ADIUS Drops	0	Client Stopp	ed Responding O	j Repea
										Refresh	Never	Show	Latest 20 record
C Re	efresh	🖨 Rese	t Repeat Co	ounts 🛛 💆 E	Export To 🕶								
	Time	Sta	Details	Ide	Endpoint ID	Endp	oint A	uthentication	n Policy	Autho	orization Policy	Authoriz	ation Profiles
	No	0	ò	user1	08:74:02:77:13	3:45 Apple-	Device D	efault >> Rule r	name ≻> Defau	ilt Defaul	lt >> NameAuthZri	ule PermitAcc	ess

Para obter mais informações, clique em **Detalhes** para ver um processo de autenticação mais detalhado.